EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Lance J. Lieberman (Reg. No. 28,437) on September 23, 2008.

1. The application has been amended as follows:

2. Claims 1, 7, 8 and 9 are amended by virtue of this Examiner's Amendment.

Claim 1 (Currently Amended):

A method of automatically classifying alerts issued by intrusion detection sensors of an information security system for producing collated alerts, each alert being defined by a plurality of qualitative attributes ($a_1,...,a_n$) belonging to a plurality of attribute domains ($A_1,...,A_n$) each of which has a partial order relationship, which method comprises the following steps:

organizing the attributes belonging to each attribute domain into a hierarchical structure including levels defined in accordance with the partial order relationship of the attribute domain, the attribute domains thus forming hierarchical structures;

constructing for each alert issued by the intrusion detection sensors ~~(11a, 11b, 11c)~~ a trellis specific to that alert by generalizing each alert in accordance with each of its attributes and at all the levels of the hierarchical structure, the specific trellis including nodes corresponding to alerts linked to each other by arcs so that each node is linked to one or more parent nodes and/or to one or more child or descendant nodes;

iteratively merging each specific trellis into a general trellis;

identifying collated alerts in the general trellis by selecting the alerts that are simultaneously the most pertinent and the most general in accordance with statistical criteria and according to their attributes belonging to lower levels of the hierarchical structures; and

supplying the collated alerts to an output unit of an alert management system in order to provide an overview of all the alerts issued by the intrusion detection sensors.

Claim 7 (Currently Amended):

A computer readable storage medium encoded with a computer program designed to execute the method according to claim 1 when it is executed by the alert management system.

Claim 8 (Currently Amended):

An alert management system for automatically classifying alerts issued by intrusion detection sensors for producing collated alerts, each alert being defined by a plurality of qualitative attributes $(a_1,...,a_n)$ belonging to a plurality of attribute domains $(A_1,...,A_n)$ each of which has a partial order relationship, which system comprises:

processor means for organizing the attributes belonging to each attribute domain into a hierarchical structure including levels defined in accordance with the partial order relationship of the attribute domain, the attribute domains thus forming hierarchical structures;

processor means for constructing for each alert issued by the intrusion detection sensors a trellis specific to that alert by generalizing each alert in accordance with each of its attributes and at all the levels of the hierarchical structure, the specific trellis including nodes corresponding to alerts linked to each other by arcs so that each node is linked to one or more parent nodes and/or to one or more child or descendant nodes;

processor means for iteratively merging each specific trellis into a general trellis;

processor means for identifying collated alerts in the general trellis by selecting the alerts that are simultaneously the most pertinent and the most general in accordance with statistical criteria and according to their attributes belonging to lower levels of the hierarchical structures; and

processor means for supplying the collated alerts to an output unit ~~(23)~~ in order to provide an overview of all alerts issued by the intrusion detection sensors.

Claim 9 (Currently Amended):

An ~~The~~ information security system comprising intrusion detection sensors and an alert management system according to claim 8.

REASONS FOR ALLOWANCE

1. Claims 1-9 are allowed.

2. The following is an examiner's statement of reasons for allowance:

3. Applicant's arguments presented in the Applicant's Remarks/Arguments (pages 7-13) are considered persuasive.

4. Regarding the rejections of claim 7 under 35 U.S.C. 101, the Applicant has amended the claim to add "computer readable storage medium" which renders the claim statutory. The rejection for this claim has accordingly been withdrawn.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
09/23/2008
Examiner, Art Unit 2131